



TECHNICAL NOTE

Creating and Using Configuration Templates



www.fortinet.com

Creating and using configuration templates

FortiManager v3.0 MR5

18 September 2007

02-30005-0430-20070919

© Copyright 2007 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Introduction

This technical note describe how to create and apply FortiGate configuration templates with the FortiManager and FortiGate units.

A configuration template is a configuration file for a specific platform and firmware build that can be applied to other similar FortiGate devices. Since the template does not contain FortiGate-specific information such as serial number, IP and host name, the template can be installed on any FortiGate device of the same model and firmware build without overwriting the new device's IP or other device-specific information. By using the template feature you are able to configure multiple FortiGate devices, of the same model and firmware build, easily and quickly.

A template is applied like a script, just like the FortiGate "Bulk CLI Import" function. When a template is installed on a FortiGate unit, the unit runs the script rather than doing a restore/reboot.

You can create templates and import them into the FortiManager central repository. Templates are visible from the central repository, as well as from the Template tab when viewing a device. Templates will appear under the Template tab of any device which matches the filtering options applied to the template (see ["To import the template and apply filters" on page 4](#)).

Templates can be deployed through the FortiManager if the devices are added in central management mode, or through the FortiGate web-based manager if the devices are added in local management mode.

Workflow for creating and applying a template

If you are setting up multiple FortiGate units of the same model at different sites, follow the process below to save time and efforts:

Common steps

The following procedures apply to the FortiGate units both in central and local modes.



Note: Unregistered devices are capable of operating in local mode.

To create the template

- 1 Start a FortiGate unit with factory defaults and save the factory defaults configuration file.
- 2 Configure the FortiGate unit as required to include all configuration you want to install to the other FortiGate units.
- 3 Save the new configuration file.
- 4 Compare the factory defaults configuration file with the modified configuration file by running a "Diff" tool.
- 5 Copy and paste the added and changed configuration items to a text editor and remove anything that is site-specific, such as IP and default route.

- 6 Save the file.

To import the template and apply filters

- 1 In the FortiManager web-based manager, go to Device Manager.
- 2 From the main toolbar, select View > All Templates.
- 3 Select Import Templates.

Name	Date/Time	Platform	Firmware Version	Created by	Comments	
test_temp	2007-09-18 10:25:31		FortiOS	admin		

- 4 Name the template, add any comments as required, and select the file created in step 6 of “To create the template” on page 3.
- 5 Optionally, select any filters to restrict the devices that are able to access the template.
- 6 Select OK.

To set unregistered device options

This is to allow the FortiManager Server to add unregistered devices to the Unregistered Devices list so that the devices can receive FortiGuard updates and access the templates.



Note: Unregistered devices are capable of operating in local mode.

- 1 In the FortiManager web-based manager, go to Device Manager.
- 2 In the navigation frame, select Unregistered Devices.
- 3 In the Unregistered Devices list, select Unregistered Device Options.

Unregistered Devices Option

Ignore all unregistered devices.

Add unregistered devices to device table, but ignore service requests.

Add unregistered devices to device table, and allow Update Manager service.

OK **Cancel**

- 4 Select Add unregistered devices to device table, and allow Update Manager service.
- 5 Select OK.

To connect the FortiGate device to the FortiManager System

- 1 From each site where you want to install a FortiGate unit, power on the unit.
- 2 Configure the IP address, default route, and any other site-specific information.
- 3 Log in to the FortiGate unit.
- 4 Go to System > Admin > Central Management to configure the FortiGate unit to be managed by the FortiManager Server.

Central Management

Enable Central Management

Type FortiManager FortiGuard Management Service

IP

Allow automatic backup of configuration on logout/timeout

Apply

- 5 Select Enable Central Management.
- 6 For Type, select FortiManager as the central management service for the FortiGate unit. Enter the IP Address of the FortiManager Server.
- 7 Select Allow automatic backup of configuration on logout/timeout to have configuration backup occur when the admin session is closed - you log out of the FortiGate unit or the admin timeout is reached.
- 8 Select Apply.

FortiGate units in local mode

This procedure is recommended for provisioning FortiGate units added to the FortiManager Server in local management mode.

The FortiGate units can be registered and unregistered.

To apply the template from the FortiGate unit

- 1 In the FortiGate unit web-based manager, go to System > Maintenance> Backup&Restore.

Backup & Restore | Revision Control | FortiGuard Center

System Configuration (Last Backup: N/A)

Backup configuration to:
 Local PC FortiManager
 Encrypt configuration file
 Password:
 Confirm:
Backup

Restore configuration from:
 Local PC FortiManager
 Filename: **Browse...**
 Password:
Restore

Partition	Active	Last Upgrade	Firmware Version
1	<input checked="" type="checkbox"/>	N/A	FGT400-3.00-FW-build552-070528
2	<input type="checkbox"/>	N/A	FGT400-3.00-FW-build550-070517 [Upload and Reboot]

Boot alternate firmware

Firmware Upgrade

Upgrade from FortiGuard network to firmware version: [Please Select]

Allow firmware downgrade

Upgrade by File: **Browse...**

OK

Advanced (Import CLI Commands, Download Debug Log)

- 2 Select FortiManager under Restore Configuration From.
- 3 Select the template.
- 4 Select Restore.

The FortiGate unit will download the template and apply the configuration script.

FortiGate units in central mode

This procedure applies if the FortiGate unit is added to the FortiManager Server in central management mode.

To add the FortiGate device to the FortiManager System

- In the FortiManager web-based manager, go to Device Manager and do one of the following:
 - In the navigation frame, select All FortiGate, then the Add Device button.
 - From the main toolbar, select Device > Add Device.
 - In the navigation frame, select Unregistered Devices, then “+” for the device you want to add.

ID	Name	Model	Connecting IP	Firmware Version	Management Mode	Mode	Status (Last Checked)
1	FG200A2907300338	Fortigate-200A	172.20.120.146	FortiOS 3.00 Interim (624)	Central	NAT/Route	(12:19 Sep 11,2007)
2	FG50012205400050	Fortigate-5001	172.20.120.162	FortiOS 3.00 MR5 (559)	Central	NAT/Route	(12:29 Sep 11,2007)
3	FGT-3000-2	Fortigate-3000	172.20.120.135	FortiOS 3.00 MR5 (559)	Local	NAT/Route	(06:46 Jun 11,2007)
4	FGT-602803030112	Fortigate-60	172.20.120.122	FortiOS 3.00 MR5 (559)	Local	NAT/Route	(06:40 Aug 9,2007)
5	FGT4002803033479	Fortigate-400	172.20.120.140	FortiOS 3.00 MR5 (552)	Local	NAT/Route	(13:21 Jun 13,2007)
6	FGT_1	Fortigate-60	172.20.120.180	FortiOS 2.80 MR7 (318)	Central	NAT/Route	(09:02 Aug 29,2007)
7	FGT_50A	Fortigate-50A	172.20.120.187	FortiOS Carrier 2.80 Interim (219)	Central	NAT/Route	(07:49 Jul 10,2007)
8	FortiGate-100A	Fortigate-100A	172.20.120.181	FortiOS Carrier 2.80 Interim (318)	Central	NAT/Route	(13:18 Jun 21,2007)
9	FortiGate-800	Fortigate-800	172.20.120.133	FortiOS 3.00 MR5 (559)	Central	NAT/Route	(07:36 Jul 19,2007)
10	FortiGate800	Fortigate-800	172.20.120.185	FortiOS Carrier 2.80 Interim (218)	Central	NAT/Route	(13:17 Jun 21,2007)

- Enter the information required and select Discover. For more information, see the *FortiManager System Administration Guide (v3.0 MR5)*.

The discovery process starts. When it completes, the Add New Device page appears. If you are adding a new device that is not operational, the discovery will fail. Select Continue Adding and enter the device information in the Discovered Information section.

- Select Add.

To apply the template from the FortiManager System

This is performed if the FortiGate unit is added to the FortiManager unit in central management mode.

- In the FortiManager web-based manager, go to Device Manager.
- From the device tree, select the device to which you want to apply the template.
- Select the Template tab.

Name	Date/Time	Platform	Firmware Version	Created by	Comments
test_temp	2007-09-18 10:25:31		FortiOS	admin	

- Select the deploy icon for the template you want to apply.
- Select OK.